The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

http://www.us-cert.gov/tlp/

DATE(S) ISSUED:

09/26/2016

SUBJECT:

Multiple Vulnerabilities in OpenSSL Could Allow for Remote Code Execution.

OVERVIEW:

Multiple vulnerabilities have been discovered in OpenSSL, the most severe of which could allow for remote code execution. OpenSSL is an open-source implementation of the SSL and TLS protocols used by a number of applications and products. SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are protocols which ensure secure communication over the Internet via encryption. Successful exploitation in the most severe of these vulnerabilities could result in the attacker executing remote code in the context of the user running the affected application. Failed exploit attempts will most likely result in denial-of-service conditions.

THREAT INTELLIGENCE:

There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:

- OpenSSL version 1.1.0a
- OpenSSL version 1.0.2i

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:
Multiple Vulnerabilities have been discovered in OpenSSL, the most severe of which could allow for remote code execution. The vulnerabilities are as follows:

- OpenSSL is prone to a remote code execution vulnerability because of a use-after-free error. Specifically, this issue occurs when the incoming message size is larger than 16k. (CVE-2016-6309)
- Any attempt to use CRLs in OpenSSL 1.0.2i will crash with a null pointer exception. (CVE-2016-7052)

Successful exploitation of the most severe of these vulnerabilities could result in the attacker executing remote code in the context of the user running the affected application. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights. Failed exploit attempts will likely result in denial of service conditions.

RECOMMENDATIONS:
The following actions should be taken:
- Apply appropriate updates provided by OpenSSL and/or applicable vendors to vulnerable systems, immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Do not use the same OpenSSL private keys across multiple systems and update OpenSSL keys periodically.

REFERENCES:
OpenSSL:
https://www.openssl.org/news/secadv/20160926.txt

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6309
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7052

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

http://www.us-cert.gov/tlp/